**PATENT**

I HEREBY CERTIFY THAT ON THE DATE SHOWN BELOW, THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, AS "EXPRESS MAIL POST OFFICE TO ADDRESSEE" MAILING LABEL NO. EQ667882269US

ON 6 SEPTEMBER 2006

Lisa L Pringle

SIGNATURE LISA L. PRINGLE

**THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| Applicant | : | Kenneth Aull |
| Serial No. | : | 10/027,944 |
| Filing Date | : | December 19, 2001 |
| For | : | REVOCATION AND UPDATING OF TOKENS IN A PUBLIC KEY INFRASTRUCTURE SYSTEM |
| Group Art Unit | : | 2132 |
| Examiner | : | Venkatanaray Perungavoor |
| Attorney Docket No. | : | NG(MS)7192 |

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**APPEAL BRIEF**

Sir:

Pursuant to the Notice of Appeal filed in this case on June 7, 2006, Appellants presents herewith their Brief on appeal.

## I. TABLE OF CONTENTS

## II. REAL PARTY IN INTEREST

The real party in interest is Northrop Grumman Corporation, as indicated by the recorded Assignment, Reel/Frame: 013751/0849.

## III. RELATED APPEAL AND INTERFERENCES

There are no related appeals or interferences.

## IV. STATUS OF CLAIMS

Claim 9-13 and 18-28 which are attached in Appendix A, are currently pending in this application. Claims 1-8 and 14-17 have been canceled. Claims 9-13 and 18-28 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,757,920 to Misra, et al. ("Misra"). Claims 13, 22, 25 and 27 stand rejected as being unpatentable over Misra in view of U.S. Patent No. 6,192,131 B1 to Geer, Jr. et al. ("Geer").

The rejection of claims 9-13 and 18-28 is appealed.

## V. STATUS OF AMENDMENTS

A response to a Final Office Action (hereinafter, "Final Rejection") issued on March 8, 2006 was filed on March 20, 2006. No amendments of the claims were filed after the Final Rejection. An Advisory Action Before Filing an Appeal Brief (hereinafter, "Advisory Action") dated May 16, 2006 was issued. The

Advisory Action indicated that the request for reconsideration set forth in the Response to the Final Rejection was considered, but did not place the application in condition for allowance.

## VI. SUMMARY OF THE CLAIMED SUBJECT MATTER

One aspect of the present invention, as recited in claim 1 is directed to a method of updating a token (130 of FIG. 1), comprising accessing a database (110 of FIG. 1) by user identification and token identification (510 of FIG 5 and Page 18, Lines 10-13), wherein the database (110 of FIG. 1) has a plurality of certificates/private keys associated with each token identification (Page 12, Line 22 to Page 13, Line 3). The method also comprises determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token (130 of FIG. 1) since the last update (540 of FIG. 5 and Page 19, Lines 1-3). The method further comprises encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token (130 of FIG. 1) using a public key associated with the token identification in the database (110 of FIG. 1) to form a download packet (550 of FIG. 5 and Page 19, Lines 4-5). The method still further comprises downloading the download packet to the token (130 of FIG. 1) (560 of FIG. 5 and Page 19, Lines 7-9). The method yet further comprises activating the

certificates/private keys in the download packet using a private key in the token (130 of FIG. 1) (580 of FIG. 5 and Page 19, Lines 9-10).

Another aspect of the present invention, as recited in claim 18 is directed to a computer program for updating a token (130 of FIG. 1) embodied on a computer readable medium and executable by a computer, comprising accessing a database (110 of FIG. 1) by user identification and token identification, wherein the database (110 of FIG. 1) has a plurality of certificates/private keys associated with each token identification (Page 12, Line 22 to Page 13, Line 3). The computer program also comprises determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token (130 of FIG. 1) since the last update (540 of FIG. 5 and Page 19, Lines 1-3). The computer program further comprises encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token (130 of FIG. 1) using a public key associated with the token identification in the database (110 of FIG. 1) to form a download packet (550 of FIG. 5 and Page 19, Lines 4-5). The computer program still further comprises downloading the download packet to the token (130 of FIG. 1) (560 of FIG. 5 and Page 19, Lines 7-9). The computer program yet even further comprises activating the certificates/private keys using a private key in the token (130 of FIG. 1) (580 of FIG. 5 and Page 19, Lines 9-10).

## VII. GROUNDS OF REJECTION TO BE REVIEW ON APPEAL

A. Whether claims 9-13 and 18-28 are anticipated by Misra?

B. Whether claims 13, 22, 25 and 27 are made obvious by Misra in view of Geer?

## VIII. ARGUMENTS FOR CLAIMS 9-13 and 18-28

### A. 35 U.S.C. §102(b) Rejection of Claims 9-13 and 18-28 as Being Anticipated by Misra

The U.S. Court of Appeal for the Federal Circuit ("Federal Circuit") has held that anticipation by a single reference requires that the single prior art reference discloses each and every element of the claimed invention, arranged as in the claim. *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730, F.2d 1452, 1458, 221 U.S.P.Q. 481, 485 (Fed. Cir. 1984).

It is respectfully submitted that the rejection of claims 13, 25 and 27 as being anticipated by Misra was made in error. It appears that claims 13, 25 and 27 were mistakenly rejected under an anticipation rejection and an obviousness rejection, wherein there are specific arguments set forth only for the obviousness rejection of claims 13, 25 and 27. Accordingly, only the obviousness rejection of claims 13, 25 and 27 will be addressed in the present Appeal Brief.

1. **The Anticipation Rejection of Claims 9 and 18**

Claims 9 and 18 are not anticipated by Misra for at least the following reasons:

a. **Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claims 9 and 18.**

Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claims 9 and 18. In the Final Rejection, the Examiner contends Column 5, Line 65 to Column 6, Line 5 and Column 6, Lines 63-67 of Misra discloses this element of claims 9 and 18 (See Final Rejection, Page 3). Applicant's representative respectfully disagrees with the Examiner's contention.

The section of Misra cited by the Examiner discloses that a digitally signed and sealed certificate is created by initially generating a hash of contents with a signed and sealed certificate (See Misra, Col. 5, Line 65-Col. 6, Line 3). The cited section of Misra also discloses that a one way hash function is used to generate the hash of contents of the digitally signed and sealed certificate (See Misra, Col. 6, Lines 3-5). Claims 9 and 18 recite encrypting all certificates/private

keys using a public key associated with a token identification in a database. As stated in Misra, the hash function is a one way function. By definition, a one way function cannot be decrypted. Conversely, the certificates/private keys encrypted with the public key recited in claims 9 and 18 can be decrypted with the public key's associated private key (the private key in the token). Thus, the hash function disclosed in Misra is a completely different type of encryption from the encrypting recited in claims 9 and 18. Therefore, the hash of the contents within the signed and sealed certificate disclosed by Misra does not correspond to the download packet recited in claims 9 and 18. Accordingly, the cited section of Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claims 9 and 18.

Additionally, the cited section of Misra discloses that a user may request to download a logon certificate to a removable storage media, such as a floppy diskette, and when the user requests to download the logon certificate, the user is prompted to supply a password (See Misra, Col 6, Lines 63-67). The cited section of Misra also discloses that a one way hash function is used to hash the password, which is used to generated an encryption key, which is used to encrypt the logon certificate (See Misra, Col. 6, Line 67-Col. 7, Line 3). The cited section of Misra further discloses that the password can be later used to

generate an encryption key that can be used to decrypt the logon certificate so that the logon certificate can be retrieved from the removable storage media (See Misra, Col. 8, Lines 27-31). Thus, the password disclosed in Misra can act as a symmetric key, that is, a key that can encrypt and decrypt the same data.

Regarding the public and private key pairs recited in claims 9 and 18, when data has been encrypted with the public key, the data can only be decrypted by a corresponding private key, and not the public key. Thus, the encrypted certificate on the removable storage media disclosed in Misra is not encrypted using public/private key encryption, but rather symmetric encryption. Therefore, the encrypted certificate disclosed in Misra does not correspond to the download packet recited in claims 9 and 18. Accordingly, the cited section of Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claims 9 and 18.

Moreover, Misra discloses that logon certificates may be created though the use of asymmetric encryption (public/private key encryption) mechanisms (See Misra, Col. 6, Lines 21-29). Misra also discloses that each domain has an associated public and private key pair (See Misra, Col. 5, Lines 31-33). Claims 9 and 18 recite encrypting all certificates/private keys using a public key associated with a token identification. Nothing in Misra discloses that any removable media,

which the Examiner alleges reads on a token (See Final Rejection, Page 3), has an associated public key. Instead, the removable media disclosed in Misra is generic (a floppy diskette). Thus, the cited section of Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claims 9 and 18. In fact, nothing in Misra discloses this element of claims 9 and 18.

**b. Misra does not disclose activating certificates/private keys in a download packet using a private key in a token, as recited in claims 9 and 18.**

Misra does not disclose activating certificates/private keys in a download packet using a private key in a token, as recited in claims 9 and 18. As stated above, the logon certificate disclosed in Misra is encrypted using a symmetric key scheme. Nothing in Misra discloses the employment of a private key during the decryption of the logon certificates in Misra. Consequently, Misra does not disclose activating certificates/private keys in a download packet using a private key in a token, as recited in claims 9 and 18.

Accordingly, for the reasons stated above, Misra does not disclose each and every element of claims 9 and 18. Therefore, Misra does not anticipate claims 9 and 18, and claims 9 and 18 should be patentable over the cited art.

Thus, it is respectfully requested that the rejection of claims 9 and 18 be withdrawn.

## 2. The Anticipation Rejection of Claims 23 and 26

Claims 23 and 26 depend from claims 9 and 18, respectively, and are patentable for at least the same reasons as claims 9 and 18, and for the reasons given herein.

**a. Misra does not disclose that activating certificates/private keys further comprises entry of a passphrase, as recited in claims 23 and 26.**

Misra does not disclose that activating certificates/private keys further comprises entry of a passphrase, as recited in claims 23 and 26. Claims 9 and 18, from which claims 23 and 26 respectively depend, recite activating certificates/private keys in a download packet using a private key in a token. Thus, claims 23 and 26 (by virtue of their dependence from claims 9 and 18, respectively) recite activating certificates/private keys by using a private key in token and entering a passphrase. Applicant's representative respectfully submits that in rejecting claims 23 and 26, the Final Rejection attempts to use the same aspect of Misra (a downloading password) that was used in the rejection of claims 9 and 18 for disclosing two separate elements recited in claims 23 and 26, namely the private key and the entry of a passphrase (See Final Rejection,

Pages 2 and 4). The Federal Circuit has held that the doctrine of claim differentiation dictates that where claims use different terms, those differences are presumed to reflect a difference in the scope of the claims. *Forest Laboratories, Inc. v. Abbot Laboratories*, 239 F.3d 1305, 1310, 57 U.S.P.Q.2d 1794 (Fed. Cir. 2001). It is respectfully submitted that if the private key and the passphrase were considered to be the same element, as contended by the Examiner, claims 23 and 26 would be superfluous.

As discussed above with respect to claims 9 and 18, from which claims 23 and 26 respectively depend, Misra discloses that the password alone can be used to decrypt the logon certificate. There is no requirement that any other entity (and particularly not a private key) is needed to decrypt the logon certificate disclosed in Misra. Accordingly, Applicant's representative respectfully submits that claims 23 and 26 have not been given independent patentable weight by the Examiner. Therefore, the rejection of claims 23 and 26 should be withdrawn.

**5. <u>The Anticipation Rejection of Claims 10-12 and 24</u>**

Claims 10-12 and 24 depend either directly or indirectly from claim 9 and are not anticipated by Misra for at least the same reasons as claim 9, and for the specific elements recited therein. Accordingly, the rejection of claims 10-12 and 24 should be withdrawn.

**6. The Anticipation Rejection of Claims 19-22 and 28**

Claims 19-22 and 28 depend either directly or indirectly from claim 18 and are not anticipated by Misra for at least the same reasons as claim 18, and for the specific elements recited therein. Accordingly, the rejection of claims 19-22 and 28 should be withdrawn.

**B. 35 U.S.C. §103(a) Rejection of Claims 13, 22, 25 and 27 as Being Unpatentable Over Misra in view of Geer**

The Federal Circuit has held that that it is insufficient to establish obviousness by showing that the separate elements existed in the prior art, absent some teaching or suggestion in the prior art to combine the elements. *Arkie Lures, Inc. v. Gene Larew Tackle, Inc.*, 119 F.3d 953, 43 U.S.P.Q.2d 1294 (Fed. Cir. 1997).

**1. The obviousness rejection of claims 13 and 22**

**a. There is no motivation to combine and modify the teachings of Misra with the teachings of Geer in the manner suggested by the Examiner with respect to claims 13 and 22.**

Applicant's representative respectfully submits that there is no motivation to combine and modify the teachings of Misra with the teachings of Geer in the manner suggested by the Examiner with respect to claims 13 and 22. Claims 13 and 22 each recite that a token is a smart card. Misra provides no teaching or

suggestion to implement smart cards. Geer provides no teaching or suggestion for the distribution of logon certificates. As stated above, the Federal Circuit has held that that it is insufficient to establish obviousness by showing that the separate elements existed in the prior art, absent some teaching or suggestion in the prior art to combine the elements. *Arkie Lures, Inc. v. Gene Larew Tackle, Inc.*, 119 F.3d 953, 43 U.S.P.Q.2d 1294 (Fed. Cir. 1997). Applicant's representative respectfully submits that without using improper hindsight, one skilled in the art would not combine and modify teachings of Misra and Geer in the manner suggested by the Examiner in the Final Rejection (See Final Rejection, Page 4).

In response to Applicant's representative's arguments regarding the motivation to combine and modify the teachings of Misra and Geer, the Examiner states that the motivation is the implementation in a standard smart card (See Final Rejection, Page 2). However, the Examiner has not set forth any reason (other than the present application) as to why one skilled in the art of smart cards would look to employ the teachings of Misra. In Misra, encrypted data is stored on non-secured removable media (a floppy diskette). In contrast, a smart card includes processing capabilities. Nothing in Misra teaches or suggests that the removable storage media should include processing capabilities. Thus, there is no motivation to combine and modify the teachings of Misra and Geer in the

manner suggested by the Examiner in the Final Rejection. Accordingly, Misra taken in view of Geer does not make claims 13 and 22 obvious.

1. **The obviousness rejection of claims 25 and 27**

**a. There is no motivation to combine and modify the teachings of Misra with the teachings of Geer in the manner suggested by the Examiner with respect to claims 25 and 27.**

Claims 25 and 27 each recite that token identification is assigned by a token manufacturer at the time the token is created and stored in a database when assigned to a user. Misra does not teach or suggest the use of tokens with a token identification. Instead, in Misra, encrypted data is stored on non-secured removable media (a floppy diskette). Geer provides no teaching or suggestion for the distribution of logon certificates. Nothing in Misra teaches or suggests that the removable storage media should include a token identification.

As stated above, the Federal Circuit has held that that it is insufficient to establish obviousness by showing that the separate elements existed in the prior art, absent some teaching or suggestion in the prior art to combine the elements. *Arkie Lures, Inc. v. Gene Larew Tackle, Inc.*, 119 F.3d 953, 43 U.S.P.Q.2d 1294 (Fed. Cir. 1997). Applicant's representative respectfully submits that without using improper hindsight, one skilled in the art would not combine and modify teachings of Misra and Geer in the manner suggested by the Examiner in the

Final Rejection (See Final Rejection, Page 4). Thus, there is no motivation to combine and modify the teachings of Misra and Geer in the manner suggested by the Examiner in the Final Rejection. Accordingly, Misra taken in view of Geer does not make claims 25 and 27 obvious.

## IX. APPENDICES

The first attached Appendix contains a copy of the claims on appeal.

The second and third Appendices have been included to comply with statutory requirements.

Please charge any deficiency or credit any overpayment in the fees for this Appeal Brief to Deposit Account No. 20-0090.

Respectfully submitted,

Christopher P. Harris
Reg. No. 43,660

TAROLLI, SUNDHEIM, COVELL
& TUMMINO, L.L.P.
1300 East Ninth Street, Suite 1700
Cleveland, Ohio 44114
(216) 621-2234
(216) 621-4072 (Facsimile)
Customer No.: 26294

## Claims Appendix

Claim 9 A method of updating a token, comprising:

accessing a database by user identification and token identification, wherein the database has a plurality of certificates/private keys associated with each token identification;

determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token since the last update;

encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token using a public key associated with the token identification in the database to form a download packet;

downloading the download packet to the token; and

activating the certificates/private keys in the download packet using a private key in the token.

Claim 10 A method as recited in claim 9, further comprising:

accessing the database by token identification to identify certificates/private keys which are expired or no longer valid; and

deleting the certificates/private keys identified which are expired or no longer valid from the token.

Claim 11 The method recited in claim 10, further comprising:

transmitting a message to the user indicating no new certificates/private keys were found in the database when determined that all certificates/private keys of the plurality of certificates/private keys have been downloaded to the token since the last update from the database.

Claim 12 The method recited in claim 11, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key.

Claim 13 The method recited in claim 12, wherein the token is a smart card.

Claim 18 A computer program for updating a token embodied on a computer readable medium and executable by a computer, comprising:

accessing a database by user identification and token identification, wherein the database has a plurality of certificates/private keys associated with each token identification;

determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token since the last update;

encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token using a public key associated with the token identification in the database to form a download packet;

downloading the download packet to the token; and

activating the certificates/private keys using a private key in the token.

Claim 19 The computer program as recited in claim 18, further comprising:

accessing the database by token identification to identify certificates/private keys which are expired or no longer valid; and

deleting the certificates/private keys identified which are expired or no longer valid from the token.

Claim 20 The computer program recited in claim 19, further comprising:

transmitting a message to the user indicating no new certificates/private keys were found in the database when determined that all certificates/private

keys of the plurality of certificates/private keys have been downloaded to the token since the last update from the database.

Claim 21 The computer program recited in claim 20, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key.

Claim 22 The computer program recited in claim 21, wherein the token is a smart card.

Claim 23 The method recited in claim 9, wherein the activating the certificates/private keys further comprises the entry of a passphrase.

Claim 24 The method recited in claim 9, further comprising:

revoking each certificate/private key associated with a selected token identification for a given token.

Claim 25 The method recited in claim 9, wherein the token identification is assigned by the token manufacturer at the time the token is created and stored in the database when assigned to a user.

Claim 26 The computer program recited in claim 18, wherein the activating occurs in response to receipt of a passphrase.

Claim 27 The computer program recited in claim 18, wherein the token identification is assigned by the token manufacturer at the time the token is created and stored in the database when assigned to a user.

Claim 28 The computer program recited in claim 18, further comprising: revoking each certificate/private key associated with a selected token identification for a given token.

## Evidence Appendix

None

## Related Proceedings Appendix

None